VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA

EKONOMICKÁ FAKULTA

KATEDRA ÚČETNICTVÍ

Elektronický podpis v účetní praxi

Electronic signature in accounting practice

Student: Patricie Kubcová

Vedoucí bakalářské práce: Ing. Marcela Palochová, Ph.D.

Ostrava 2010

„Místopřísežně prohlašuji, že jsem celou práci vypracovala samostatně“.

V Ostravě dne ……. podpis…….

Děkuji Ing. Marcele Palochové za její odborné vedení, diskuze a připomínky, které napomohly ke zpracování této bakalářské práce.

Obsah

1 Úvod

Elektronický podpis v účetní praxi je velmi aktuálním tématem současnosti. V dnešní době si lze jen obtížně představit efektivní komunikaci podniků bez využití informačních technologií, jehož nedílnou součástí je právě i elektronický podpis.

Pokrok ve vývoji informačních technologií byl jednoznačně přínosem jak pro podniky, tak i pro jiné uživatele. Jako nejvýznamnější přínos a zjednodušení při používání elektronického podpisu lze označit fakt, že uživatelé uspoří mnoho času a zefektivní komunikaci podniků se svým okolím, ať už se jedná o komunikaci se státní správou či obchodními partnery.

Cílem bakalářské práce je přiblížení problematiky týkající se elektronického podpisu jako takového a především poukázání na možnosti využití této technologie pro potřeby podnikatelských subjektů.

Cílem první kapitoly jsou nezbytně nutné obecné definice používané terminologie, která bezprostředně souvisí danou problematikou. Dalším cílem je obecné vymezení elektronického podpisu z pohledu legislativní úpravy v České republice a Evropské unii.

Cílem druhé kapitoly je vymezení základní podstaty elektronického podpisu, jíž je kryptografie. Dalším cílem kapitoly je stručná charakteristika akreditovaných certifikačních autorit v České republice a jejich porovnání. Životní cyklus certifikátu, jeho pořízení, zneplatnění a obnova je popsána v závěru kapitoly.

Poslední cíl bakalářské práce předkládá konkrétní případy využitelnosti elektronického podpisu v účetní praxi. Dále je zde vysvětlena problematika datových schránek.

2 Obecné vymezení elektronického podpisu

Elektronický podpis či zaručený elektronický podpis se používá především v internetovém prostředí k uzavírání obchodních a kupních smluv mezi obchodními partnery, při podepisování elektronických formulářů, ve veřejné či státní správě, v elektronickém bankovnictví a v jiných oblastech. Počet organizací, které jsou připraveny přijmout elektronicky podepsaný dokument, se navíc neustále zvyšuje.

Elektronický podpis je jedním z nástrojů bezpečné elektronické komunikace. Podstatou je nahrazení klasického podpisu na papíru podpisem elektronického dokumentu, při současném zachování nebo dokonce zvýšení bezpečnosti celé podpisové operace.

Pro další detailnější rozbor elektronického podpisu je nutné definovat některé používané pojmy.

Identifikace – se používá k jednoznačnému určení osoby (identity).

U fyzické osoby nepodnikající jsou předmětem identifikace následující znaky:

- všechna jména a příjmení,
- rodné číslo, a nebylo-li přiděleno, datum narození,
- místo narození,
- pohlaví,
- trvalý nebo jiný pobyt,
- státní občanství.

U fyzické osoby podnikající je třeba k výše uvedenému doplnit i obchodní firmu, odlišující dodatek nebo další označení, místo podnikání a identifikační číslo.

U právnické osoby jsou předmětem identifikace:

- obchodní firma nebo název včetně odlišujícího dodatku nebo dalšího označení,

- sídlo,
- identifikační číslo nebo obdobné číslo přidělované v zahraničí,
- u osob, které jsou jejím statutárním orgánem nebo jeho členem, údaje fyzické osoby nepodnikající (viz výše) pokud je statutárním orgánem nebo jeho členem právnická osoba, pak údaje podle tohoto odstavce.

Autentizace – je proces ověřování identity subjektu. Proběhne-li proces autentizace, dojde k autorizaci. Autentizace je bezpečnostní opatření, kterým se zajišťuje ochrana před falšováním identity, z čehož vyplývá, že jde o ověřování pravosti, hodnověrnosti. Pro zjištění identity se používají tyto základní metody:

- podle toho, co uživatel zná (zná správnou kombinaci uživatelského označení a hesla nebo PIN),
- podle toho, co uživatel má (nějaký technický prostředek, který uživatel vlastní – USB dongle, smart card, privátní klíč apod.),
- podle toho, čím uživatel je (uživatel má biometrické vlastnosti, které lze prověřit – otisk prstu, snímek oční duhovky či sítnice apod.),
- podle toho, co uživatel umí (umí správně odpovědět na náhodně vygenerovaný kontrolní dotaz).

Autenticita – je vlastnost daného subjektu, u kterého je možné ověřit identitu.

Autorizace – je úřední oprávnění, schválení či pověření. Proces autorizace označuje získání přístupu k informacím, funkcím a dalším objektům, který se skládá z autentizace subjektu (zjištění jeho identity), vyhledávání v seznamu oprávněných subjektů, jejich rolí a práv, udělení oprávnění nebo odepření přístupu.

Integrita – dodržení integrity znamená požadavek na prokázání, že po podpisu nedošlo k žádné změně či úpravě dat v souboru.

2.1 Elektronický podpis v ČR

V České Republice byl roku 2000 přijat zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů dále jen „zákon o elektronickém podpisu“. Tento zákon byl přínosem nejen pro ulehčení komunikace a úspory času, ale také snížil míru nákladů (např. poštovné).

Zákon upravuje v souladu s právem Evropských společenství používání elektronického podpisu, elektronické značky, poskytování certifikačních služeb a souvisejících služeb poskytovateli, usazenými na území České republiky, kontrolu povinností stanovených tímto zákonem a sankce za porušení povinností stanovených tímto zákonem.

Elektronický podpis - podle zákona o elektronickém podpisu se jedná o údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě. [4]

Zaručený elektronický podpis - jím se dle zákona rozumí elektronický podpis, který splňuje následující požadavky:

- je jednoznačně spojen s podepisující osobou,
- umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
- byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
- je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat. [4]

Elektronická značka – jsou údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a splňují následující požadavky:

- jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu,

- byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou,
- jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat. [4]

Datová zpráva – to jsou elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou. [4]

Podepisující osoba – je fyzická osoba, která je držitelem prostředků pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby. [4]

Označující osoba – může být fyzická osoba, právnická osoba nebo organizační složka státu, která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou. [4]

Kvalifikované časové razítko – je datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb. Důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem. [4]

Elektronická podatelna – pracoviště orgánu veřejné správy určené pro příjem a odesílání datových zpráv.

V § 3 zákona o elektronickém podpisu se uvádí, že datová zpráva je podepsána, pokud je označena elektronickým podpisem založeným na kvalifikovaném certifikátu a vytvořeným pomocí prostředku pro bezpečné vytváření

podpisu. To umožňuje ověřit, že datovou zprávu podepsala osoba uvedená na tomto kvalifikovaném podpisu. [4]

V § 5 zákona o elektronickém podpisu jsou uvedeny povinnosti podepisující osoby, a to tyto:

- podepisující osoba je povinna zacházet s prostředky, jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití;
- uvědomit neprodleně poskytovatele certifikačních služeb, který vydal kvalifikovaný certifikát, o tom, že hrozí nebezpečí zneužití jejích dat pro vytváření zaručeného elektronického podpisu. [4]

Za škodu způsobenou porušením základních povinností odpovídá podepisující osoba podle zvláštních právních předpisů. Odpovědnosti se však zprostí, pokud prokáže, že ten, komu vznikla škoda, neprovedl veškeré úkony potřebné k tomu, aby si ověřil, že zaručený elektronický podpis je platný a jeho kvalifikovaný certifikát nebyl zneplatněn. [1]

Elektronický podpis je dále upraven vyhláškou Úřadu pro ochranu osobních údajů č. 366/2001 Sb. Tato vyhláška upravuje způsob, jakým se dokládá splnění povinností poskytovatelů certifikačních služeb, požadavky na nástroje elektronických podpisů a náležitosti postupu a způsobu vyhodnocování souladu nástrojů elektronického podpisu s těmito požadavky. [4]

2.2 Elektronický podpis v EU

Evropský parlament a Rada Evropské unie přijaly dne 13.12. 1999 směrnici 1999/93/ES o zásadách Společenství pro elektronické podpisy, dále jen „směrnice“.

Tato směrnice byla přijata, aby usnadnila používání elektronických podpisů a přispěla k jejich právnímu uznání. Stanovuje taktéž právní rámec pro elektronické podpisy a některé ověřovací služby.

Dle této směrnice by měly členské státy zajistit dohled nad tím, aby elektronickým podpisům nebyla upírána právní účinnost a aby nebyly odmítány jako důkazy v soudním řízení.

Členské státy mají povinnost oznámit Komisi Evropské unie a ostatním členským státům informace o dobrovolných akreditačních systémech na vnitrostátní úrovni, názvy a sídla vnitrostátních subjektů odpovědných za akreditaci a dohled, názvy a sídla všech vnitrostátních akreditovaných ověřovatelů.

Komisi Evropské unie napomáhá Výbor pro elektronické podpisy s kontrolou této problematiky. Ten má vlastní jednací řád a dohlíží na dodržování vnitřních principů při jednotném vnitřním trhu a přijímání elektronického podpisu. [17]

2.3 Druhy elektronických podpisů

V našich podmínkách existují dvě varianty elektronického podepisování a to:

- konstantní podpis – identifikátor uživatele + přístupové heslo, což nepředstavuje prakticky žádnou ochranu proti sofistikovanějšímu útoku;
- proměnlivý podpis – tzv. zaručený elektronický podpis, má vyšší úroveň bezpečnosti jelikož musí splňovat následující požadavky:
  - je jednoznačně spojen s podepisující osobou,
  - umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
  - byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
  - je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat. [3]

3 Podstata a fungování elektronického podpisu

Elektronický podpis je vytvořen na základě kryptografie, neboli šifrování, což je nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí.

3.1 Základy kryptografie

Kryptografie, tedy nauka o šifrovaní, tvoří jednu z teoreticky i prakticky nejlepších metod ochrany údajů. Historicky se vyvinula jako metoda ochrany údajů při jejich přenosu, avšak toto zabezpečení lze použít i na zašifrování údajů, které se uchovávají pouze na jednom místě. Moderní kryptografie kromě tohoto základního použití zahrnuje i různé aplikace základních kryptografických algoritmů, jako jsou například digitální podpisy, nebo speciální protokoly pro zabezpečení elektronických platebních systémů, které jsou nevyhnutelné například pro komerční využití internetu.

Šifrování se může poměrně volně chápat jako jistá transformace originálních údajů, které je potřeba chránit, a to tak že se převedou do jiného tvaru. Z hlediska bezpečnosti je důležité, aby pouze určený subjekt dokázal zpětně dešifrovat text. Šifrovací systém se považuje za bezpečný, když se údaje mohou dešifrovat jen se speciální znalostí – dešifrovacího klíče. [1]

Pro bezpečnou a důvěryhodnou komunikaci v souladu s mezinárodními normami se definují základní bezpečnostní cíle, které je zajišťují:

- **důvěrnost informací** – systém musí zabezpečit, aby přístup k důvěrným informacím měly pouze autorizované subjekty, tedy ty, kterým je zpráva určena,
- **integritu** – systém musí zabezpečit informace proti modifikaci, změně přenášených dat,
- **nepopiratelnost** – systém musí mít schopnost přesvědčit třetí nezávislou stranu o přímé odpovědnosti subjektu za autorství, vlastnictví,

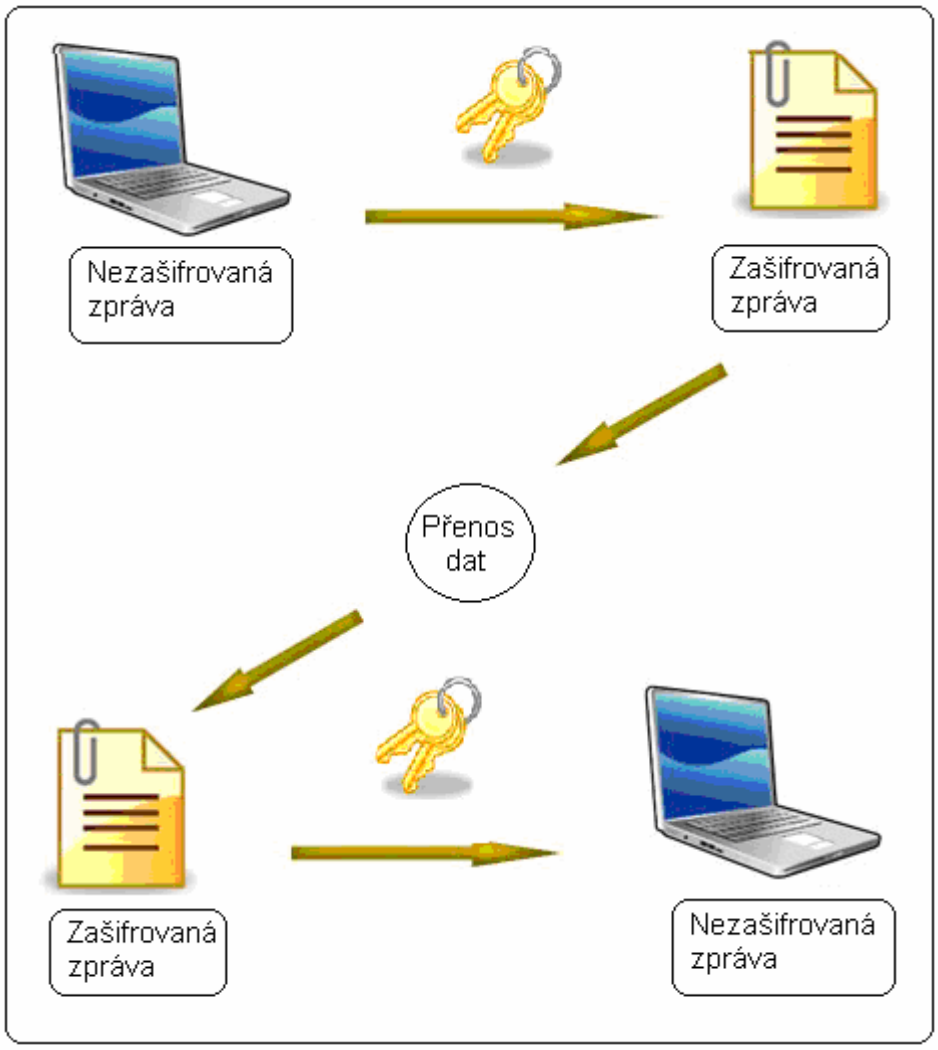
odeslání, případně přijetí zprávy. Tento bezpečnostní atribut lze chápat jako vyšší formu autentizace.

Ochranu informací lze rozdělit do dvou základních oblastí, symetrickou kryptografii a asymetrickou kryptografii, jejíž podmnožinou je kryptografie s veřejným klíčem.[1]

3.1.1 Symetrická kryptografie

Symetrické šifrování je na rozdíl od asymetrického šifrování postavené jen na jednom klíči, který se nazývá tajný klíč, ten slouží nejen na zašifrování odeslané zprávy, ale zároveň i na dešifrování přijaté zprávy, z čehož vyplývá potřeba obeznámit příjemce s tímto klíčem, aby mohl zprávu bez problémů dešifrovat. Tento klíč je tedy společným tajemstvím komunikujících stran. Předání tajného klíče se může uskutečnit buď osobním předáním, nebo zasláním tajného klíče prostřednictvím důvěryhodného kanálu. Existuje tu však dosti značné riziko odcizení tajného klíče třetí stranou. [1]

Obr. 3.1 Šifrování zpráv symetrickou šifrou



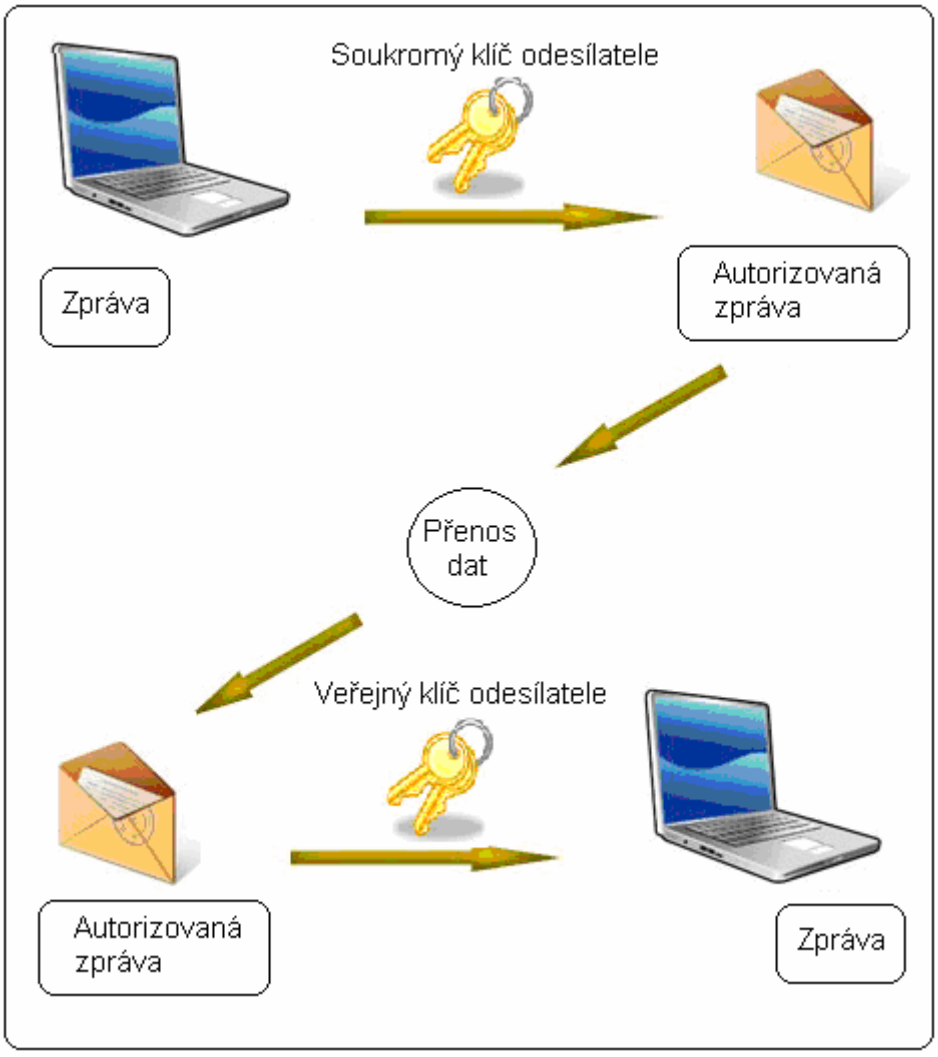
Zdroj: vlastní zpracování

3.1.2 Asymetrická kryptografie, kryptografie s veřejným klíčem

Asymetrické šifrování zvyšuje bezpečnost šifrování využíváním dvou odlišných, ale matematicky souvisejících klíčů známých pod názvy veřejný klíč a soukromý klíč. Pokud lze jeden z klíčů zveřejnit – veřejný klíč, aniž by bylo možné z něj v reálném čase odvodit druhý klíč – soukromý klíč, označuje se taková kryptografie jako kryptografie s veřejným klíčem. Data, která jsou šifrována jedním z těchto klíčů lze reálně dešifrovat v rozumném čase pouze se znalostí klíče druhého. [1]

Přenos autorizované zprávy – soukromý klíč je s maximální možnou mírou chráněn majitelem (soukromý klíč) a druhý klíč je zveřejněn (veřejný klíč). Zprávu odesilatel zašifruje svým soukromým klíčem a příjemce ji dešifruje pouze jediným klíčem veřejným (odpovídající danému soukromému klíči). Příjemce zná vlastníka tohoto klíče, a proto zná jednoznačně odesilatele zprávy. Protože však veřejný klíč není důvěrný, není ani zpráva důvěrnou. Zprávu si může přečíst kdokoli, ale je autorizovaná, nepopiratelná (podepsaná), odesilatel nemůže odmítnout odpovědnost. [1]

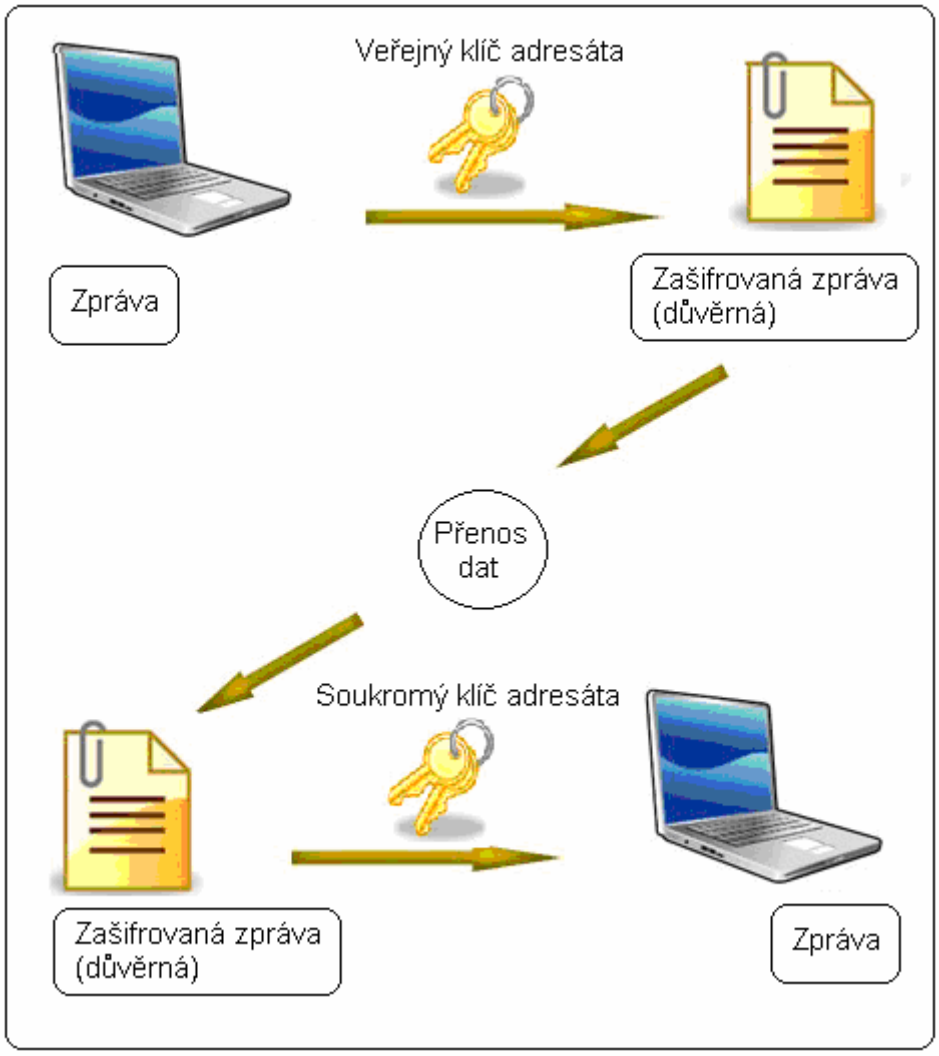
Obr. 3.2 Přenos neadresované, nezašifrované (veřejné), ale autorizované zprávy



Zdroj: vlastní zpracování

Přenos neautorizované, ale zašifrované (důvěrné) zprávy – pro zajištění důvěrnosti zprávy je třeba užití opačného postupu šifrování. Zpráva je zašifrována veřejným klíčem a jediný, kdo ji dokáže dešifrovat a přečíst, je majitel soukromého klíče. Tímto je zajištěna ochrana zprávy – její důvěrnost. Není však autorizována – podepsána (veřejný klíč je všem dostupný a zprávu mohl zašifrovat kdokoli). [1]

Obr. 3.3 Přenos adresované, zašifrované (důvěrné), ale neautorizované zprávy

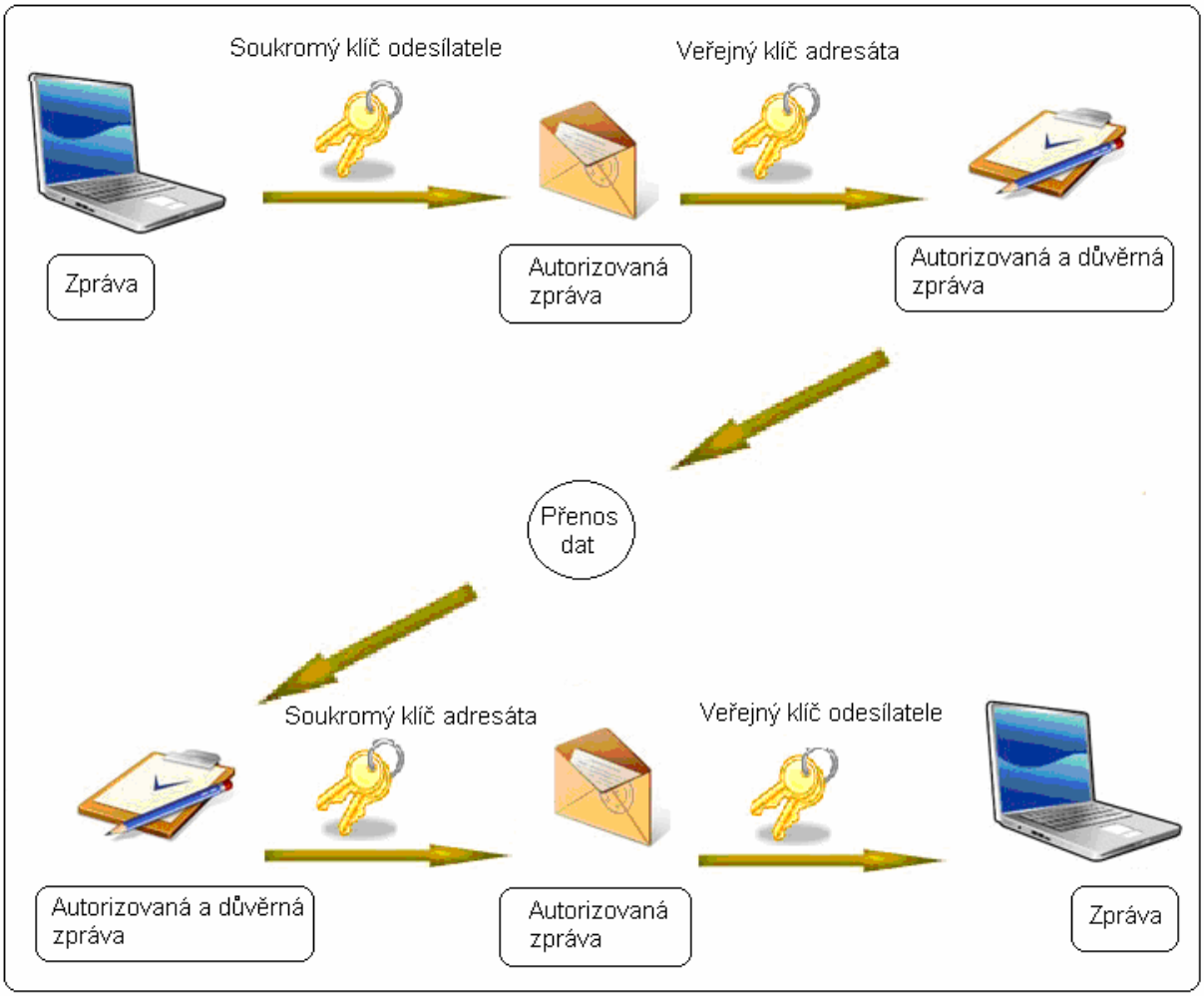


Zdroj: vlastní zpracování

Přenos zašifrované a zároveň autorizované (podepsané zprávy) – metoda používá oba výše uvedené postupy zároveň. Zpráva je odesílatelem nejprve podepsána – autorizována prostřednictvím jeho soukromého klíče, dále použije veřejný klíč příjemce k zašifrování a tedy zajištění důvěrnosti = čitelnosti pouze pro

příjemce. Příjemce po přijetí zprávu nejprve dešifruje svým soukromým klíčem a následně si ověří identitu odesilatele tak, že zprávu dešifruje veřejným klíčem odesilatele. [1]

Obr. 3.4 Přenos adresované, zašifrované (důvěrné) a autorizované zprávy.



Zdroj: vlastní zpracování

Složitost asymetrického šifrování je příčinou pomalejšího procesu šifrování. Studie ukázaly, že symetrické šifrování je minimálně stokrát rychlejší než asymetrické šifrování v případě, když jsou použité na šifrování softwarové prostředky a dokonce až desettisíckrát rychlejší při použití hardwarových prostředků. [1]

3.2 Certifikační autorita

Elektronický podpis se v některých případech stává důvěryhodným, když je založen na certifikátu. Elektronický podpis je v takovém případě pro každou podepsanou zprávu jiný a odvozuje se od této zprávy. Právě takovýto podpis se nazývá zaručeným elektronickým podpisem, který je v jistých situacích vyžadován při komunikaci s veřejnou správou i jinými subjekty. Certifikát lze získat od poskytovatele **certifikačních služeb (certifikační autority)**. Pro ověření úplnosti, správnosti a pravdivosti uváděných údajů je vyžadována osobní návštěva na některém registračním místě certifikační autority.

Certifikační autorita plní dvě základní funkce:

- Certifikační - zaručující, že deklarovaný veřejný klíč přísluší dané osobě, jedná se o vydání certifikátů uživatelům, který potvrzuje, že veřejný klíč uvedený na certifikátu patří jednoznačně dané osobě. Certifikát zároveň obsahuje další informace týkající se uživatele, doby platnosti klíče, informace o používání klíče a informace o certifikační autoritě. Certifikát je podepsán elektronickým podpisem certifikační autority;
- Validační – certifikační autorita potvrzuje uživateli platnost certifikátu jejího partnera. [5]

Vydávání kvalifikovaných certifikátů je podmíněno rozhodnutím Úřadu pro ochranu osobních údajů, tento úřad ve svém Věstníku vydává přehled akreditovaných poskytovatelů certifikačních služeb vydávajících kvalifikované certifikáty. V současné době oprávnění vydávat kvalifikované certifikáty mají tři subjekty a to:

- První certifikační autorita, a. s.,
- eIdentity, a. s.,
- PostSignum QCA (služba České pošty, s. p.).

3.2.1 První certifikační autorita, a. s. (I.CA)

Certifikační autorita I.CA zahájila poskytování svých služeb v roce 1996. Tato společnost převzala od mateřské společnosti veškeré činnosti, které bezprostředně souvisí s poskytováním certifikačních služeb. Akreditace pro výkon činnosti akreditovaného poskytovatele certifikačních služeb byla udělena 15. 3. 2002. V současnosti je společnost vlastněna několika významnými společnostmi, a to:

- Česká spořitelna, a.s.
- Československá obchodní banka, a.s.
- Telefónica O2 Czech Republic, a.s.
- Asseco, a.s.
- Státní tiskárna cenin s.p.

I.CA je oprávněna poskytovat kvalifikované certifikační služby nejen v oblasti kvalifikovaných certifikátů, ale i v oblastech kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek, k tomuto získala akreditaci 1. 2. 2006.

I.CA je v současnosti největším poskytovatelem komplexních služeb vydávání a správy certifikátů v České republice. Svoje služby poskytuje také na Slovensku. Počty vydaných certifikátů jsou dnes evidovány řádově ve statisících.

Služby a produkty, které I.CA v současné době poskytuje jsou následující:

- Kvalifikovaný certifikát – kvalifikovaný certifikát využijí všichni občané, firmy, úřady. Vhodný je pro komunikaci občanů se státní správou a samosprávou, stejně jako pro komerční aplikace. Používání tohoto certifikátu znamená výraznou časovou úsporu a volnost. Z technologického pohledu lze tento certifikát využít k vytváření a ověřování elektronických podpisů a zajištění neodmítnutelnosti odpovědnosti;
- Komerční certifikát – použití vhodné v uzavřených systémech, mezi účastníky bezpečné komunikace. Další využití je možné tam, kde nelze podle současné legislativy kvalifikované certifikáty použít, a to pro šifrování a autentizaci;

- TWINS – je to kombinace kvalifikovaného a komerčního certifikátu. Uživatel může využívat službu elektronického podpisu a zároveň služby autentizace a šifrování;
- e-Já – v podstatě se jedná o TWINS uložený na bezpečném mediu s bezpečným přístupem, což umožňuje přenášet „elektronickou totožnost“ mezi různými počítači;
- Komerční certifikát pro server – je určen pro bezpečnou komunikaci serverů;
- Kvalifikovaný systémový certifikát – je určen k bezpečnému ověření elektronických značek. Tento certifikát lze použít na vytváření a ověřování elektronických značek, bezpečné ověřování elektronických značek, zajištění neodmítnutelnosti odpovědnosti;
- Testovací certifikát – především slouží k ověření funkčnosti technologie použité pro realizaci tvorby elektronického podpisu. Testovací certifikát je vždy vydáván zdarma. [15]

3.2.2 eIdentity, a. s.

Společnost eIdentity a. s. vznikla na počátku roku 2004, již na počátku své činnosti se orientovala na komplexní služby v oblasti správy elektronické identity. Jako akreditovaný poskytovatel certifikačních služeb působí do září 2005, kdy získala akreditaci.

Produkty, které poskytuje eIdentity jsou následující:

akreditované služby

- vydání kvalifikovaného certifikátu,
- vydání kvalifikovaného certifikátu s vyznačením identifikátoru ministerstva práce a sociálních věcí,
- vydání kvalifikovaného certifikátu s vyznačením pracovní pozice v organizaci,
- vydání kvalifikovaného systémového certifikátu.

komerční služby

- vydání komerčního certifikátu pro elektronický podpis,
- vydání komerčního certifikátu pro šifrování zpráv,
- vydání komerčního certifikátu pro identifikaci,
- vydání komerčního serverového certifikátu pro SSL/TLS. [10]

3.2.3 PostSignum QCA

Česká pošta, s. p. se stala akreditovaným poskytovatelem certifikačních služeb dne 3. 8. 2005 na základě akreditace udělené Ministerstvem informatiky ČR. Certifikační autorita PostSignum QCA rozšiřuje obchodní aktivity České pošty, s. p. o služby vydávání kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů.

Produkty poskytované PostSignum QCA:

- certifikáty pro ověření elektronického podpisu zaměstnance,
- certifikáty organizace pro ověření elektronické značky,
- certifikáty pro ověření elektronického podpisu fyzické osoby,
- certifikáty pro ověření elektronické značky fyzické osoby. [14]

3.2.4 Porovnání akreditovaných poskytovatelů certifikačních služeb

Při výběru poskytovatele certifikačních služeb se zájemce o elektronický podpis zaměří zejména na jednotlivé oblasti, jako jsou potřebné dokumenty při vydání certifikátu, doba použitelnosti certifikátu, doba zpracování žádosti o certifikát a jeho vydání a v neposlední řadě cena poskytovaných služeb.

Potřebné dokumenty při vydání certifikátu

Akreditovaní poskytovatelé certifikačních služeb (I.CA, eIdentity a PostSignum) mají v podstatě totožné požadavky na identifikaci osob při prvotní žádosti o certifikát.

Před vydáním certifikátu musí certifikační autorita ověřit identitu osob, které žádají o certifikát. U první žádosti se identifikace provádí doložením příslušných dokladů:

- ověřování identity u právnické osoby nebo organizační složky státu – certifikační autorita vyžaduje originál nebo notářsky ověřenou kopii výpisu z obchodního rejstříku, nebo jiného zákonem určeného registru, živnostenský list, zřizovací listinu (ty musí obsahovat úplné obchodní jméno, identifikační číslo, adresu sídla, jména osob oprávněných k zastupování a způsob jakým za právnickou osobu jednají a podepisují);
- doklady předkládané na registrační autoritě fyzickou osobou nepodnikající – občanský průkaz (nebo obdobný doklad stejné právní váhy) a osobní doklad který je vydán orgánem veřejné moci nebo jinou organizací, jejíž existenci lze doložit (řidičský průkaz);
- u osoby samostatně výdělečně činné nebo u zaměstnance se předkládají – stejné doklady jako u fyzických osob nepodnikajících a potvrzení o zaměstnaneckém poměru k danému zaměstnavateli.

Při vydání již druhotného certifikátu postačí, aby žádost byla podepsána ještě platným elektronickým podpisem.

Žádost o certifikát může podat každá fyzická osoba, která je způsobilá k právním úkonům.

Z uvedeného vyplývá, že toto hledisko nemá žádný dopad při rozhodování osoby či subjektu, kterého poskytovatele certifikačních služeb zvolí.

Doba zpracování žádosti o certifikát a jeho vydání

Doba zpracování žádosti o certifikát se u jednotlivých poskytovatelů mírně liší, avšak žádný z poskytovatelů nestanovuje pevný časový limit, jelikož tato doba je

závislá především na žadateli. Pro vydání prvotního certifikátu je nezbytně nutná osobní návštěva u registrační autority.

- I.CA uvádí dobu vydání certifikátu do patnácti minut,
- eIdentity - stanovuje lhůtu pro vyzvednutí certifikátu do třiceti dnů od zaplacení, pokud se žadatel v tomto termínu nedostaví nebo si nedohodne schůzku, je žádost zrušena,
- PostSignum - do dvou pracovních dnů od podání žádosti posoudí a vydá rozhodnutí o vydání certifikátu, po tomto rozhodnutí je poskytovatel povinen vydat certifikát do následujícího pracovního dne.

Při rozhodování může tedy napomoci tento faktor. Nejrychlejší vydání certifikátu má jednoznačně I.CA.

Cena poskytovaných služeb

Poskytovatelé certifikačních služeb se velmi výrazně liší v cenách za vydávané certifikáty. V následujících tabulkách jsou uvedeny ceny za poskytované certifikáty jednotlivých poskytovatelů certifikačních služeb. [10] [14] [15]

Tab. 3.3 I.CA – ceník za poskytované služby

	Typ certifikátu	Platnost certifikátu	Cena certifikátu včetně DPH
Kvalifikované certifikáty	Standard	12 měsíců	495,- Kč
	Comfort	12 měsíců	Prvotní certifikát 1 230,- Kč Následný certifikát 495,- Kč
Kvalifikované systémové certifikáty	Standard	12 měsíců	780,- Kč
	Comfort	12 měsíců	Prvotní certifikát 1 515,- Kč Následný certifikát 780,- Kč
	Kvalifikovaný podpisový certifikát ke kvalifikovanému systémovému certifikátu	12 měsíců	390,- Kč
Komerční certifikáty	Standard	12 měsíců	395,- Kč
	Comfort	12 měsíců	Prvotní certifikát 1 130,- Kč Následný certifikát 395,- Kč
	Certifikát pro server	12 měsíců	1 170,- Kč

Zdroj: vlastní zpracování

Tab. 3.1 eIdentity - ceník za poskytované služby

	Typ certifikátu	Platnost certifikátu	Cena certifikátu včetně DPH
Akreditované služby	Kvalifikovaný certifikát	12 měsíců	395,- Kč
	Kvalifikovaný systémový certifikát	12 měsíců	3 480,- Kč
Komerční služby	Komerční certifikát	12 měsíců	354,- Kč
	Komerční serverový certifikát	12 měsíců	1 074,- Kč
Balíčky služeb	Balíček kvalifikovaného certifikátu a k němu vydaného komerčního certifikátu	12 měsíců	750,- Kč
	Balíček kvalifikovaného systémového certifikátu a k němu vydaného komerčního serverového certifikátu	12 měsíců	3 858,- Kč

Zdroj: vlastní pracování

Tab. 3.2 PostSignum – ceník za poskytované služby

Vydávané certifikáty	Platnost certifikátu	Cena certifikátu včetně DPH
Certifikáty pro ověření elektronického podpisu zaměstnance	12 měsíců	190 Kč
Certifikáty organizace pro ověření elektronické značky	12 měsíců	2856 Kč
Certifikáty pro ověření elektronického podpisu fyzické osoby	12 měsíců	190 Kč
Certifikáty pro ověření elektronické značky fyzické osoby	12 měsíců	2856 Kč

Zdroj: vlastní zpracování

Z uvedených tabulek je zřejmé, že z finančního hlediska jsou poskytované služby snadno dostupné. Všechny vydávané certifikáty mají platnost 12 měsíců, takže toto hledisko je při rozhodování bezpředmětné. Záleží tedy na každém pořizovateli, jakého poskytovatele certifikačních služeb si zvolí.

3.3 Životní cyklus certifikátu

Vydaný certifikát má omezenou dobu platnosti, na každém certifikátu se nachází jeho platnost. Hlavním důvodem omezené doby platnosti certifikátu je pokrok ve zvyšování výkonnosti výpočetní techniky a potenciální možnost objevení mezer v protokolech nebo algoritmech, tímto by se mohly certifikáty ve dlouhodobém časovém horizontu stát nespolehlivými.

3.3.1 Postup získávání certifikátu

Tvorba certifikátu se skládá z následujících úkonů:

a) generování šifrovacích klíčů a žádosti o certifikát - jedná se o data k vytváření a ověřování elektronického podpisu, výsledkem tohoto procesu je elektronický dokument (žádost o certifikát),

b) příprava identifikačních dat - žadatel o certifikát shromáždí osobní identifikační materiály nutné pro vydání certifikátu, jako jsou například IČ, DIČ, číslo občanského průkazu a podobně,

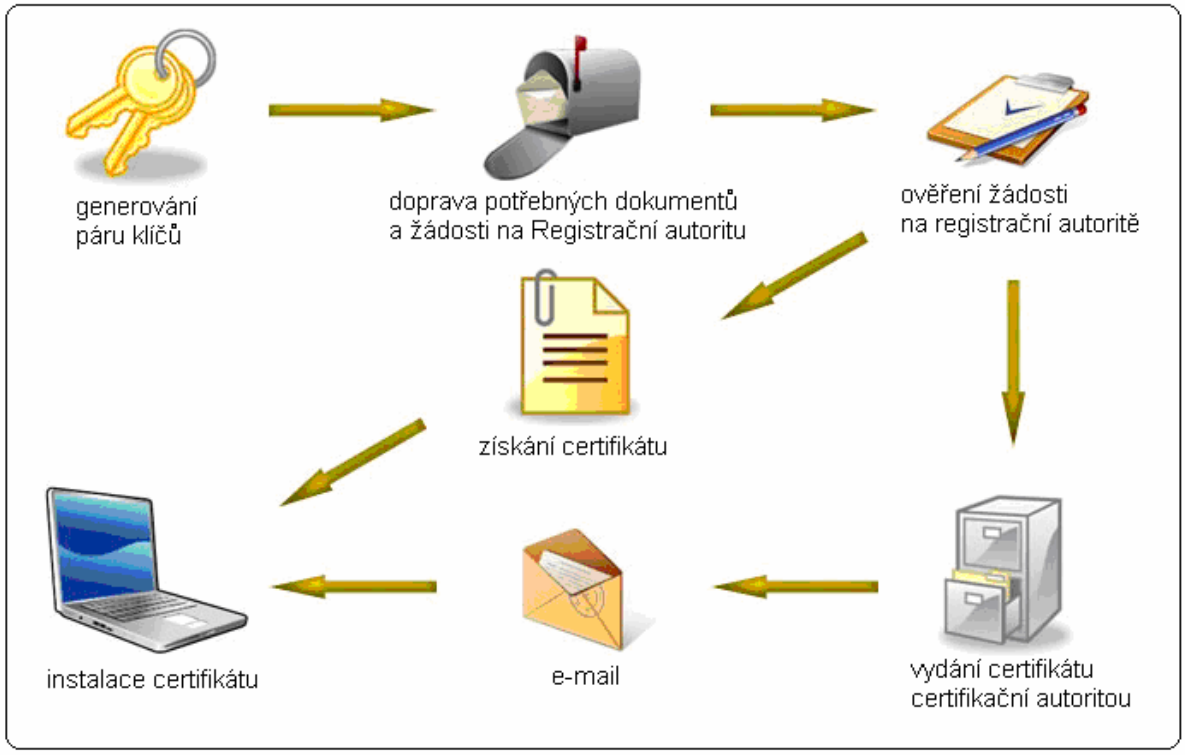
c) předání žádosti o certifikát certifikační autoritě – kontaktní místa certifikační autority se nazývají registrační autority, zde žadatel předá data nutná k vydání certifikátu spolu s doklady o jejich pravosti,

d) ověření informací – certifikační autorita ověřuje, zda může certifikát žadateli vydat nebo lze ověřit konzistenci dat pro vytváření a ověřování elektronického podpisu a jejich jedinečnost v rámci konkrétní certifikační autority,

e) tvorba certifikátu – certifikační autorita vytvoří elektronický dokument příslušného formátu a ten následně elektronicky podepíše,

f) předání certifikátu – podle dohody je certifikát žadateli předán, zaslán či zveřejněn. [2]

Obr. 3.5 Proces získání certifikátu



Zdroj: www.ica.cz

3.3.2 Instalace certifikátu

Certifikáty je možné nainstalovat pouze na počítači, kde byly vygenerovány klíče a žádosti o certifikát, které žadatel předkládal na obchodním místě při sepisování konkrétní smlouvy. Při instalaci je dále důležité dát si pozor na uživatelská práva, vše musí být nainstalováno na stejném uživatelském účtu v počítači, na kterém došlo ke generování klíčů a žádosti o certifikát. Jakmile jsou certifikáty nainstalovány je nutné provést zálohu, nejlépe na přenosné médium. Pokud totiž dojde k vážné poruše na počítači a původní certifikát je zničen, lze díky této záloze certifikát i nadále používat. Další možností je žádost o zneplatnění certifikátu a vydání nového certifikátu. [14]

3.3.3 Zneplatnění certifikátu

Zneplatnění certifikátu je mimořádná situace, při které se předčasně ukončí platnost certifikátu. Nejčastější důvod pro zrušení certifikátu je obava z vyzrazení soukromého klíče. Zneplatnit certifikát lze několika způsoby, ať už se jedná o osobní návštěvu na registrační autoritě, pomocí e-mailu či pomocí formuláře na webu konkrétní certifikační autority. Je nutná identifikace žadatele, aby nedošlo ke zneužití potenciálním útočníkem.

Každá certifikační autorita vede veřejně přístupný seznam zneplatněných certifikátů, jejichž doba platnosti ještě nevypršela. Tento seznam je aktualizován v pravidelných intervalech. Certifikáty jsou v tomto seznamu vedeny až do řádného vypršení jejich platnosti. [1]

3.3.4 Obnova certifikátu

Jak již bylo zmíněno, certifikáty mají časově omezenou platnost, zpravidla jeden rok, to znamená, že po uplynutí této doby by bylo nutné opět generovat žádost o certifikát a dostavit se k certifikační autoritě s potřebnými doklady pro vydání nového certifikátu. Řešením úspory času je obnova certifikátu, který se dá získat bez osobní návštěvy certifikační autority. Tato obnova certifikátu má však několik podmínek. Hlavní podmínkou je to, že se z pohledu osobních dat klienta nic nezměnilo. Druhou, neméně důležitou podmínkou je obnova certifikátu v době platnosti prvotního certifikátu. Certifikační autorita potřebuje jednoznačně autentizovat a autorizovat žadatele o následný certifikát.

V praxi je obvyklé, že certifikační autorita pošle klientům e-mail s upozorněním o konci platnosti certifikátu. Tento e-mail obsahuje popis postupu obnovy certifikátu. Při obnově certifikátu se generuje nová žádost o certifikát, nelze použít žádost z prvotního certifikátu, jelikož certifikační autorita požaduje nový pár klíčů. Vyplněná žádost se odešle na certifikační autoritu, kde je zpracována. Po ověření elektronického podpisu ve zprávě a celkové kontrole žádosti vydá certifikační autorita následný certifikát. [1]

3.3.5 Archivace elektronických dokumentů

Používání informačních technologií je spojeno se vznikem nové problematiky ověřování a dokládání pravosti a neměnnosti dokumentů v elektronické podobě v delším časovém horizontu.

Možnost použití zaručeného elektronického podpisu zajistí integritu a autenticitu takového dokumentu v okamžiku jeho přijetí. Díky takovémuto označení se elektronický dokument stává právně nezpochybnitelným, avšak pouze po dobu platnosti certifikátu. [16]

Elektronické archivy a systémy pro správu dokumentů musí splnit určité podmínky, aby tyto dokumenty byly právně nezpochybnitelné. Mezi tyto podmínky patří:

- uchovávané dokumenty musí obsahovat svůj elektronický podpis,
- jako hlavní prostředek doložení existence dokumentu v čase slouží kvalifikované časové razítko,
- dokumenty musí být po celou dobu archivace v nezměněném stavu, včetně elektronických podpisů a časových razítek (to je zabezpečeno automatickým mechanismem – před vypršením platnosti certifikátu se obnoví platnost časového razítka),
- v případě potřeby dokázání autenticity dokumentu se vygeneruje důkazní záznam. [16]

Důkazní záznam slouží k prokázání, že daný dokument existoval v nezměněné podobě v daném časovém období.

4 Využití elektronického podpisu v účetní praxi

Elektronická komunikace je základním a nezbytným předpokladem pro efektivní komunikaci firmy se svým okolím, ať už se jedná o komunikaci s obchodními partnery či orgány veřejné správy. Díky technologii elektronického podpisu se dá efektivněji využít čas, nemusí se stát fronty na úřadech a řešit případné konflikty plynoucí z osobního jednání. Tento uspořený čas by se mohl využít k získávání nových obchodních partnerů či zakázek.

4.1 Komunikace s orgány veřejné správy

Pro elektronickou komunikaci s orgány veřejné správy je jednoznačně nutná legislativní úprava. Úřady nemohou samy zavést žádnou elektronizaci bez jasného vymezení v zákonech. V České republice je použití elektronizace úřady veřejné správy vymezena následujícími právními předpisy:

- zákon č. 227/2000 Sb., o elektronickém podpisu;
- vyhláška č. 496/2004 Sb., k elektronickým podatelnám;
- nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů;
- vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb;
- zákon 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. [11]

Možností pro využití elektronického podpisu ve vztahu k veřejné správě je celá řada, příkladem jsou elektronické podatelny a datové schránky.

Elektronické podatelny

V zákoně o elektronickém podpisu je elektronická podatelna definována jako pracoviště orgánu veřejné moci určené pro příjem a odesílání datových zpráv. Funkci podatelny však detailněji definuje vyhláška č. 496/2004 Sb., k elektronickým

podatelnám. Tato vyhláška stanoví postupy orgánů veřejné moci uplatňované při přijímání a odesílání datových zpráv prostřednictvím elektronické podatelny a strukturu údajů kvalifikovaného certifikátu, na základě kterých je možné podepisující osobu při přijímání datových zpráv prostřednictvím elektronické podatelny jednoznačně identifikovat. [4]

Datové schránky

Datová schránka je elektronické úložiště, které slouží k doručování dokumentů orgánů veřejné moci a provádění úkonů vůči veřejné moci. Datová schránka je povinná pro právnické osoby zřízené zákonem, právnické osoby zapsané v obchodním rejstříku a orgány veřejné moci. Ostatní právnické osoby, fyzické osoby či podnikající fyzické osoby si mohou dobrovolně datovou schránku také zřídit. Samotná aktivace datové schránky je zcela bezplatná, pouze vyřízení elektronického podpisu je zpoplatněno. [4]

Daňová informační schránka

Daňová informační schránka slouží k poskytování informací z elektronických spisů, vedených daňovou správou, pro autorizované uživatele. Pro možnost používání daňové informační schránky je nutné si zažádat o zřízení daňové identifikační schránky a podat si přihlášku k nahlížení do této schránky, to lze pouze s použitím zaručeného elektronického podpisu. [8]

4.1.1 Ministerstvo financí

Pro komunikaci s finančními úřady lze využívat EPO – elektronické podání pro daňovou správu. Prostřednictvím České daňové správy leze podávat následující formuláře:

- souhrnné hlášení VIES;
- přiznání k dani z přidané hodnoty;
- daň z příjmů fyzických osob;

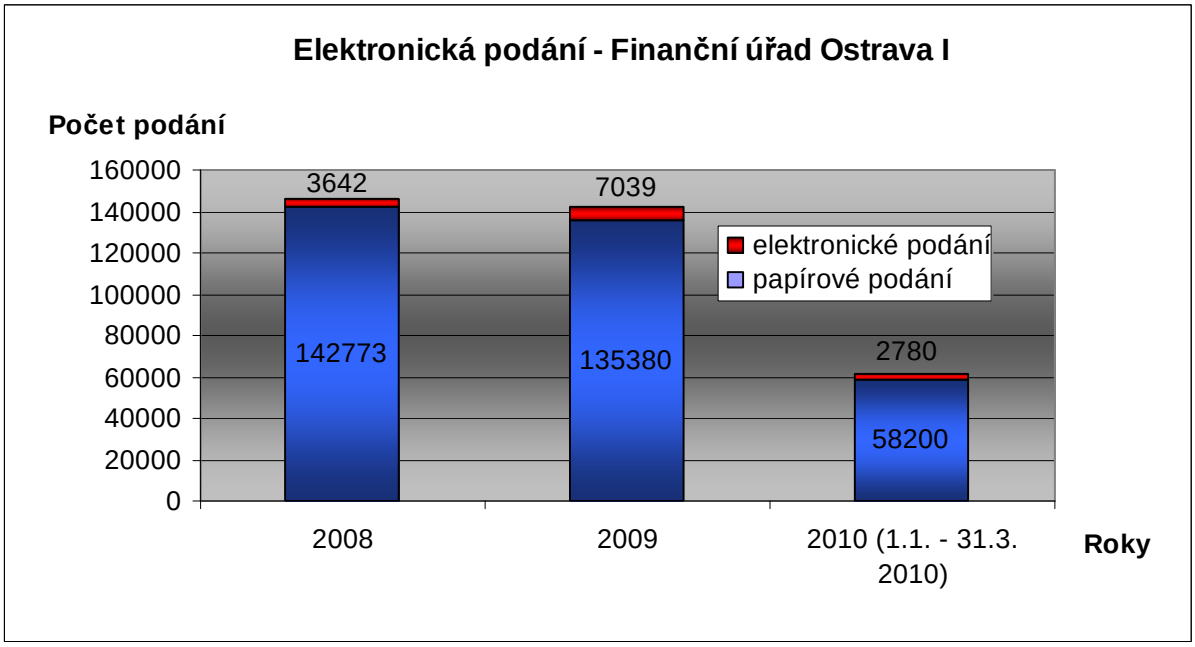
- daň z příjmů právnických osob;
- vyúčtování daně z příjmů fyzických osob ze závislé činnosti a funkčních požitků včetně všech příloh;
- daňové přiznání k dani silniční;
- daňové přiznání k dani z nemovitostí;
- oznámení o nezdaněných vyplácených částkách fyzickým osobám;
- obecná písemnost určená pro podání státních orgánů a bank;
- obecná písemnost určená pro finanční úřad, finanční ředitelství nebo Ministerstvo financí;
- hlášení platebního zprostředkovatele podle § 38fa zákona 586/1992 Sb.;
- plná moc;
- plná moc neomezená. [6]

Podání lze uskutečnit prostřednictvím internetu nebo na přenosném médiu – disketě. Při podání přes internet lze uskutečnit podání jako podání s datovou zprávou se zaručeným elektronickým podpisem nebo jako podání s datovou zprávou bez zaručeného elektronického podpisu. V případě, že je podání s datovou zprávou bez zaručeného elektronického podání je vyžadováno podání v písemné podobě.

Pro vyjádření vývoje využívanosti elektronického podpisu ve vztahu k finančním úřadům byly získány údaje od Finančního úřadu pro Ostravu I. Jedná se tedy o prezentaci místního využití. Hodnoty se mohou lišit od hodnot v rámci celé České republiky.

Využití elektronické komunikace ve vztahu k Finančnímu úřadu Ostrava I dokládají následující grafy.

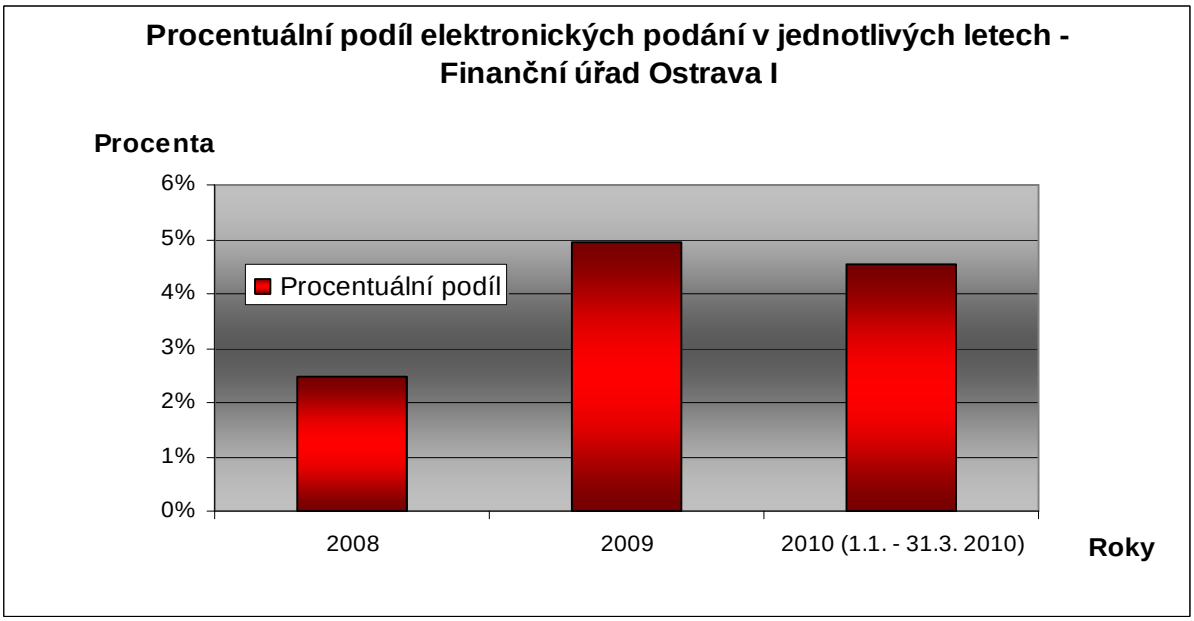
Graf 4.1 Elektronická podání – Finanční úřad Ostrava I



Zdroj: vlastní zpracování

Z uvedeného grafu (Graf 4.1) je zřejmé, že papírové podání je výrazně preferovanější než podání elektronické. Následující graf (Graf 4.2) však ilustruje rostoucí procentuální podíl elektronických podání.

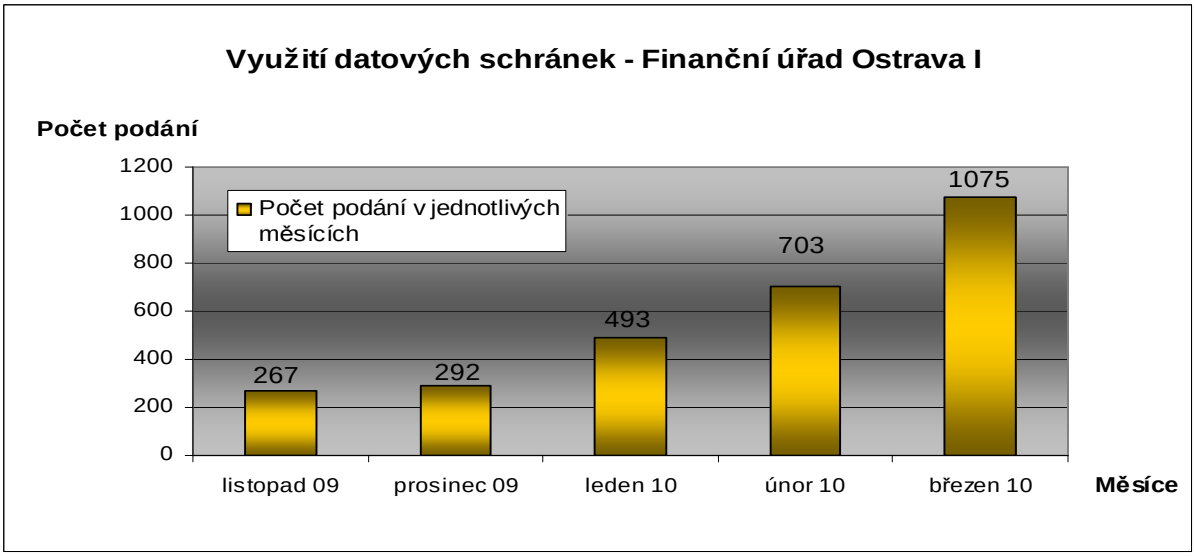
Graf 4.2 Procentuální podíl elektronických podání – Finanční úřad Ostrava I



Zdroj: vlastní zpracování

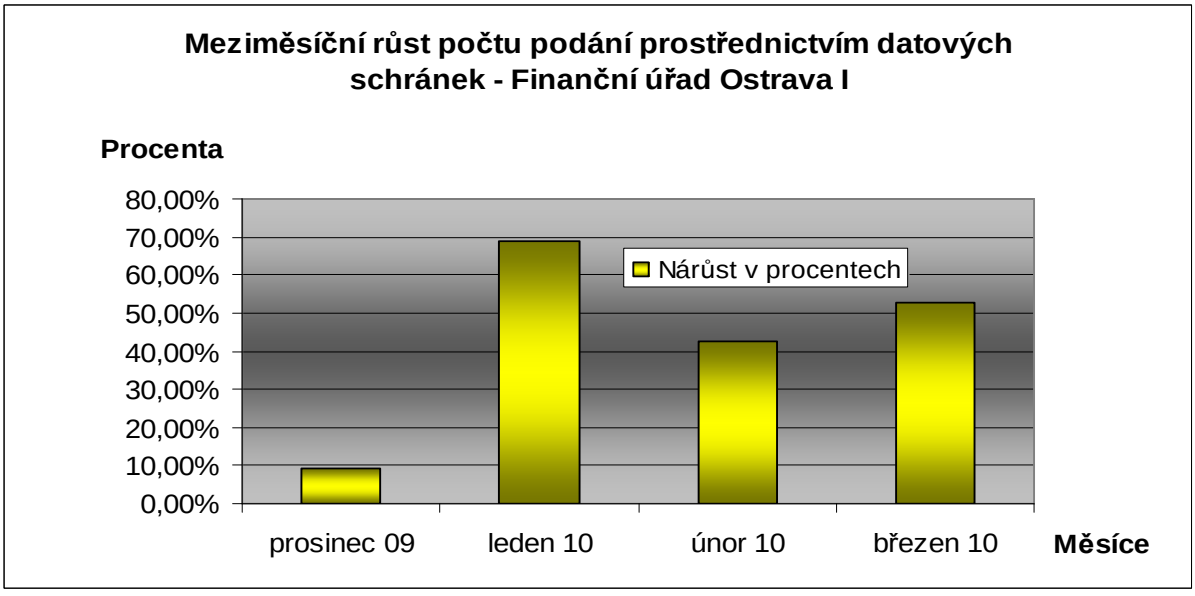
Od zavedení datových schránek v listopadu 2009, se jejich používání zvyšuje, což dokládá graf 4.3. V následujícím grafu (Grafu 4.4) je vyjádřen meziměsíční růst podání pomocí datových schránek.

Graf 4.3 Využití datových schránek 2009/2010 – Finanční úřad Ostrava I



Zdroj: vlastní zpracování

Graf 4.4 Meziměsíční růst počtu podání prostřednictvím datových schránek – Finanční úřad Ostrava I

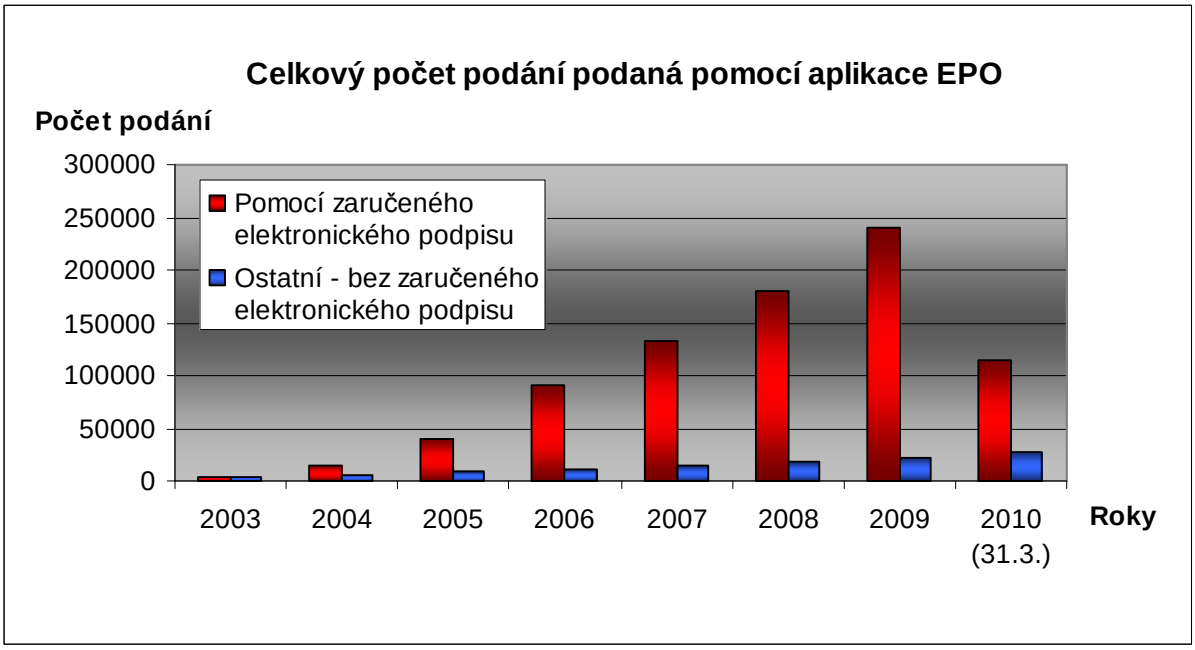


Zdroj: vlastní zpracování

Z grafů je zřejmé, že využívání datových schránek i elektronických podatelen se zvyšuje.

Využívání elektronického podání dokládá také graf 4.5 a tabulka 4.1, ve kterých se nacházejí počty elektronických podání uskutečněných prostřednictvím aplikace elektronického podání na portálu České daňové správy za celou Českou republiku. Graf předkládá souhrn veškerých podání, v tabulce jsou pak uvedeny jednotlivé dílčí typy písemností.

Graf 4.5 Celkový počet podání podaná pomocí elektronického podání



Zdroj: vlastní zpracování

Tab. 4.1 Počet elektronických podání uskutečněných prostřednictvím elektronického podání

Typ písemnosti (Typ podání)		Rok							
		2003	2004	2005	2006	2007	2008	2009	2010 (31.3.)
Daň z nemovitostí	ZAREP	460	396	703	961	1 264	1 813	2 308	2 327
	Ost	325	374	1 070	1 257	1 621	2 332	2 001	3 865
Daň z přidané hodnoty	ZAREP	3 353	10 162	26 965	53 122	77 342	102 777	134 256	43 331
	Ost	1 773	3 360	4 742	5 410	7 010	7 777	10 673	3 669
Souhrnné hlášení VIES	ZAREP	0	290	1 410	2 931	4 615	6 224	8 246	15 457
	Ost	0	121	325	414	456	498	714	10 017
Daň silniční	ZAREP	14	899	2 185	4 830	7 577	10 123	12 561	15 103
	Ost	789	901	1 077	1 671	1 459	1 634	1 690	2 205
Daň z příjmů fyzických osob	ZAREP	0	172	1 495	3 105	5 573	8 217	10 454	3 549
	Ost	0	21	1 009	2 149	3 619	5 628	4 858	5 893
Daň z příjmů právnických osob	ZAREP	0	182	1 243	2 613	4 670	6 674	9 314	2 349
	Ost	0	24	260	289	411	554	716	743
Oznámení podle § 34 zákona č.337/1992 Sb.	ZAREP	0	4	83	80	158	172	201	250
	Ost	71	13	26	40	68	70	85	83
Hlášení platebního zprostředkovatele	ZAREP	0	0	0	50	134	133	106	9 975
	Ost	0	0	0	116	123	59	58	55
Vyúčtování daně z příjmů fyzických osob	ZAREP	0	0	0	1 158	2 736	4 188	5 755	26
	Ost	0	0	0	112	387	530	536	7 788
Žádost o zřízení/zrušení DIS	ZAREP	0	0	0	5 243	5 625	6 110	7 034	961
Přihlášení ke službám daňového portálu	ZAREP	0	0	0	4 842	5 225	6 148	7 131	2 063

Obecná písemnost určená pro FÚ, FŘ nebo MF	ZAREP	233	3 286	6 385	12 473	17 196	24 561	34 200	2 186
Obecná písemnost určená pro podání státních orgánů a bank	ZAREP	0	0	0	0	0	2 740	8 516	3 426
Žádost o přidělení přístupu do Aplikace pro vrácení DPH plátcům v jiných členských státech	ZAREP	0	0	0	0	0	0	12	1 032
Žádost o vrácení DPH do jiných zemí EU	ZAREP	0	0	0	0	0	0	0	386
Žádost o vrácení DPH z jiných zemí EU	ZAREP	0	0	0	0	0	0	0	466
Daň vybíraná srážkou	ZAREP	0	0	0	0	0	0	1	5 134
	Ost	0	0	0	0	0	0	0	659
Celkem	ZAREP	4 060	15 391	40 469	91 408	132 115	179 880	240 705	114 877
	Ost	2 958	4 814	8 509	11 458	15 154	19 082	21 331	28 121

Zdroj: http://cds.mfcr.cz/cps/rde/xchg/cds/xsl/dane_elektronicky_416.html?year=0

Vysvětlivky:

ZAREP – podání se zaručeným elektronickým podpisem čili kvalifikovaným certifikátem

Ost – podání bez zaručeného elektronického podpisu.

4.1.2 Česká správa sociálního zabezpečení

Česká správa sociálního zabezpečení od roku 2004 přijímá elektronické formuláře prostřednictvím e-Podání. E-Podání není elektronickou podatelnou České správy sociálního zabezpečení, je specifickým informačním kanálem, kterým se dostávají data od klientů do informačních systémů prostřednictvím Portálu veřejné správy. To musí obsahovat zaručený elektronický podpis na základě kvalifikovaného certifikátu a musí být zašifrována platným šifrovacím certifikátem České správy sociálního zabezpečení. Takto zabezpečenými formuláři mohou být například:

- evidenční listy důchodového pojištění;
- potvrzení o studiu/ o teoretické a praktické přípravě;
- oznámení o nástupu do zaměstnání;
- přehled o příjmech a výdajích osob samostatně výdělečně činných;
- přehled o výši pojistného. [7]

Komunikovat s Českou správou sociálního zabezpečení lze i prostřednictvím Portálu veřejné správy, jak bylo zmíněno výše, kde se používá aplikace Elektronické podání. Toto aplikace umožňuje jednoduchou komunikaci s různými úřady veřejné správy. Pro práci v aplikaci je však nutná registrace, která není nikterak složitá. [13]

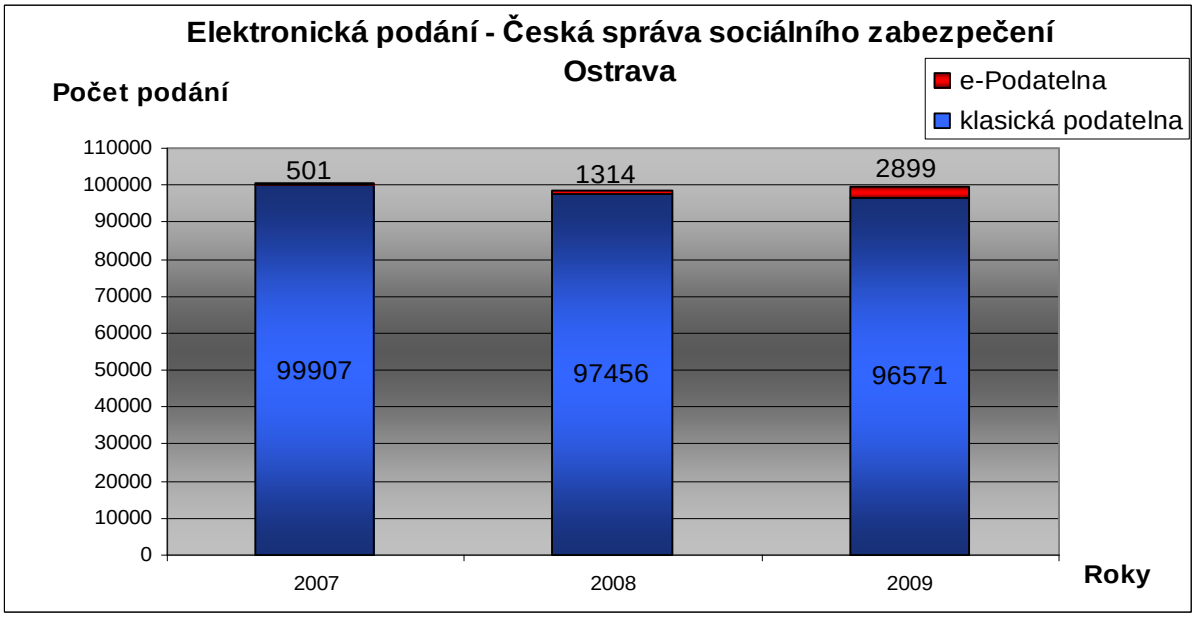
Pro praktické poukázání na vývoj elektronické komunikace s Českou správou sociálního zabezpečení byly použity údaje z Okresní správy sociálního zabezpečení Ostrava.

Používání elektronické komunikace ve vztahu k České správě sociálního zabezpečení Ostrava dokládají následující grafy.

V grafu 4.6 je zobrazeno využití e-podatelen a klasických podatelen, u klasické podatelny jsou zahrnuty i došlé vlastní písemnosti. Na druhou stranu se zde neuvádějí písemnosti došlé obyčejnou zásilkou, ke kterým není nutná odpověď, jako jsou například formuláře.

Opět je zde využití klasické podatelny zřetelně vyšší než u e-podatelny. Avšak následující graf (Graf 4.7) poukazuje na rostoucí využívanost.

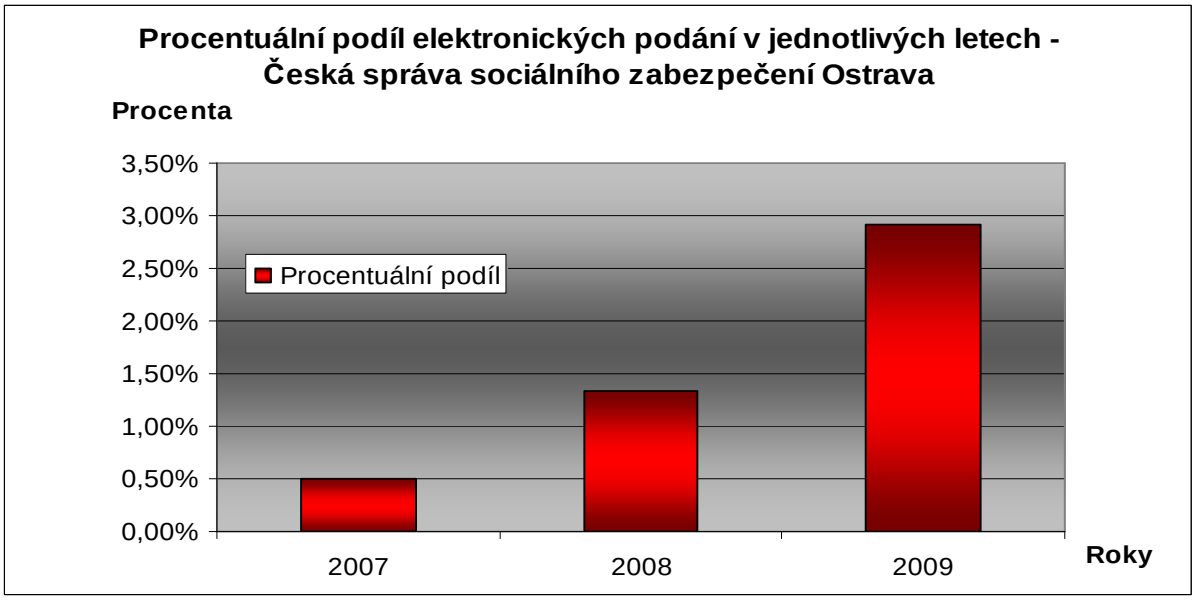
Graf 4.6 Elektronická podání – Česká správa sociálního zabezpečení



Zdroj: vlastní zpracování

V dalším grafu (4.7) je vyjádřen procentuální růst elektronické komunikace ve vztahu k České správě sociálního zabezpečení Ostrava.

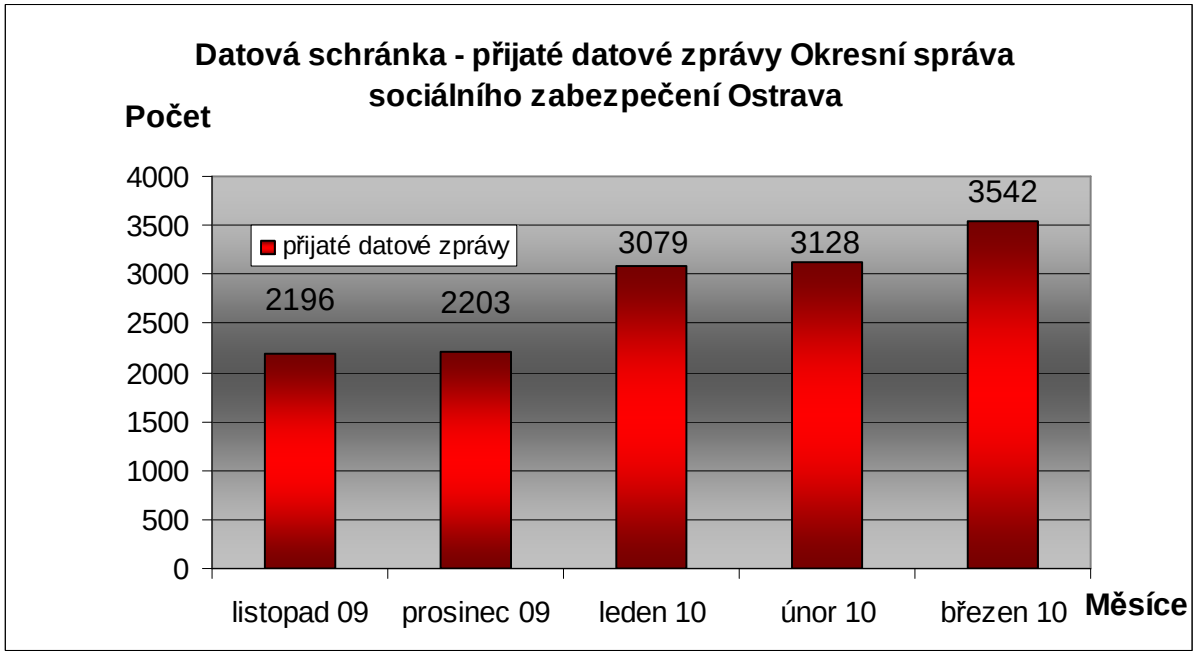
Graf 4.7 Procentuální podíl elektronických podání – Česká správa sociálního zabezpečení Ostrava



Zdroj: vlastní zpracování

Při komunikaci pomocí datových schránek ve vztahu k České správě sociálního zabezpečení Ostrava je složení následující. Graf 4.8 předkládá počet přijatých datových zpráv, přičemž přibližně 95 % došlých podání jsou od okresních a krajských soudů, Magistrátu města Ostravy, Policie, exekutorů zbylých 5 % podání je od ostatních subjektů.

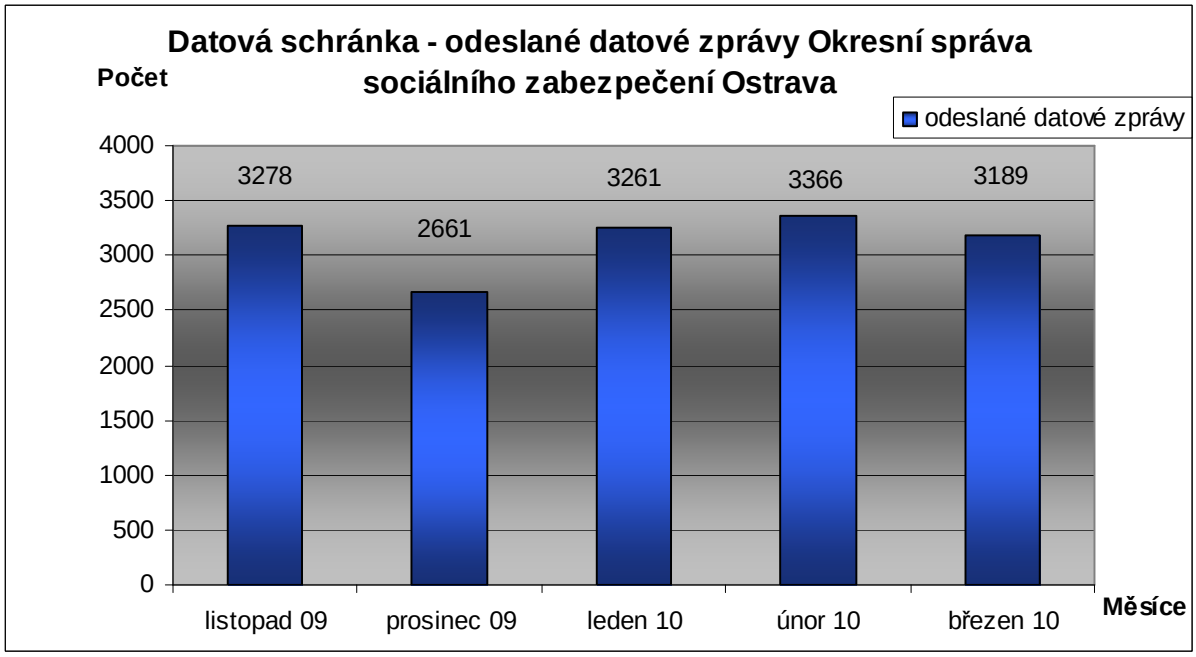
Graf 4.8 Využití datových schránek Okresní správou sociálního zabezpečení Ostrava – přijaté datové zprávy



Zdroj: vlastní zpracování

V případě odesílání datových zpráv je situace vyjádřena v grafu 4.9, přičemž přibližně 60 % datových zpráv je určeno zpětně okresním a krajským soudům, Magistrátu města Ostravy, Policii a exekutorům. Zbylých 40 % zpráv je pro zaměstnavatele a peněžní ústavy.

Graf 4.9 Využití datových schránek Okresní správou sociálního zabezpečení Ostrava – odeslané datové zprávy



Zdroj: vlastní zpracování

4.2 Elektronická výměna dat – EDI

Elektronická výměna dat patří mezi moderní způsoby komunikace mezi dvěma nezávislými subjekty. Zajišťuje výměnu standardizovaných obchodních dokumentů, jako jsou objednávky, faktury či dodací listy přímo mezi informačními systémy obchodních partnerů, i když tito partneři používají jiné podnikové systémy. Jednoduše řečeno, objednávka pořízena v informačním systému odběratele se automaticky přenese do informačního systému dodavatele, aniž by se musela do informačního systému ručně přepisovat. Cílem elektronické výměny dat je nahrazení papírových dokumentů elektronickými, čímž se snižují náklady a zvyšuje se efektivita a kvalita prováděných postupů, přičemž právní váhu mají naprosto stejnou jako standardní papírové dokumenty.

Elektronická výměna dat se dá také chápat jako sada standardů pro strukturování informací s cílem výměny dat mezi danými subjekty, tyto standardy popisují struktury dokumentů.

Mezi hlavní výhody zavedení elektronické výměny dat do společnosti se může uvést následující:

- snižuje náklady za poštovné, tisk, evidenci, administrativu;
- šetří čas – zrychluje tok dokumentů;
- zjednodušuje předávání dokladů a jejich archivaci;
- omezuje chybovost při ručním zadávání dat;
- zvyšuje bezpečnost předávaných dokumentů;
- možnost napojení na elektronický platební styk;
- integrita – po celou dobu existence dokladu je zajištěna nezměnitelnost obsahu;
- autenticita – věrohodnost původu je zajištěna elektronickým podpisem a šifrováním;
- zkvalitňuje vztahy mezi obchodními partnery;
- umožňuje jednotnou komunikaci rozdílných systémů a subjektů;
- přispívá k efektivnějšímu plánování a řízení výroby a obchodu;
- umožňuje dokonalejší zásobování a strategické plánování dodávek.

Vzájemná komunikace spolupracujících systémů je zajištěna používáním mezinárodního standardu, který se označuje UN/EDIFACT. EDIFACT je obecná a mezioborová norma, v rámci které vznikají jednotlivé aplikační normy pro konkrétní odvětví, jako jsou například obchod, doprava, státní správa, bankovnictví či automobilový průmysl.

EDIFACT je nejlépe propracovaný standard, má více než sto typů zpráv. Mezi nejpoužívanější typy zpráv lze zařadit následující:

- potvrzení o převzetí zprávy;
- obchodní námitka;
- kontrolní zpráva;
- avízo o odeslání zboží;

- avízo příchodu zásilky;
- faktura;
- přehled zásob;
- objednávka;
- informace o organizaci;
- katalog zboží a cen;
- potvrzení příjmu zboží;
- avízo o platbě;
- oznámení o vrácení zboží. [9]

Jedním z nejvýznamnějších a nejčastěji používaných dokumentů v účetnictví je jednoznačně faktura. Z tohoto titulu je žádoucí se o využitelnosti tohoto typu zprávy blíže seznámit.

Obecně faktura je daňovým dokladem, má tedy předepsané náležitosti. Pokud neobsahuje všechny předepsané náležitosti, nejedná se už o daňový doklad.

Mezi předepsané náležitosti běžného daňového dokladu patří:

- označení kupujícího a prodávajícího (obchodní firma nebo jméno a příjmení, název a dodatek ke jménu, sídlo, místo podnikání plátce, daňové identifikační číslo);
- evidenční číslo daňového dokladu;
- rozsah a předmět plnění;
- datum vystavení daňového dokladu;
- datum uskutečnění zdanitelného plnění nebo datum přijetí úplaty;
- jednotkovou cenu bez daně;
- základ daně;
- sazbu daně (snížená 10 % nebo základní 20 %);
- výši daně (uvedenou v české měně). [4]

Pro možnost využití daňových dokladů je však vyžadováno splnění dvou podmínek stanovených zákonem č. 235/2004 Sb. o dani z přidané hodnoty.

První podmínkou je nutný souhlas příjemce faktury, že je ochoten a schopen elektronickou fakturu přijmout. Příjemce takovéto faktury musí mít k dispozici odpovídající prostředky pro jejich příjem, otevření a následnou archivaci. To zajistí odpovídající software.

Druhou podmínkou je opatřit tento daňový doklad zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb. [12]

5 Závěr

V dnešní době je technologie elektronického podpisu takřka nepostradatelná, jeho využití se uplatní zejména při komunikaci například s finančními úřady, Českou správou sociálního zabezpečení a dalšími subjekty.

Elektronický podpis je pro svou relativně nízkou cenu, rychlé pořízení a mnohostranné použití velmi zdařilou službou. Náklady spojené s předáváním papírových dokumentů, ať obchodním partnerům či ve vztahu k veřejné správě, mnohonásobně převyšují náklady na pořízení zaručeného elektronického podpisu.

Závěry plynoucí z analýzy provedené v bakalářské práci říkají, že elektronická komunikace s veřejnou správou pomocí zaručeného elektronického podpisu každoročně narůstá. Obdobný rostoucí trend má i využití nově zavedeného institutu datových schránek. Díky přijatelné ceně a nenáročnosti pořízení prostředků pro využití elektronického podpisu využívají mimo podniky tuto technologii i živnostníci a občané.

Cíle bakalářské práce byly naplněny v hlavních vymezených bodech jako seznámení se s problematikou elektronického podpisu, poukázání na možnosti využití této technologie, rozsah praktické realizace a rozvíjející se oblasti využití v České republice. Úžeji pak byl vyčíslen podíl využití této technologie ve vztahu k Finančnímu úřadu pro Ostravu I., České správě sociálního zabezpečení a vývojové tendence do budoucna.

Seznam použité literatury:

Odborná literatura:

[1] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi*. 1. vyd. Olomouc: ANAG, 2008. 160 s. ISBN 978-80-7263-465-1.

[2] LIDINSKÝ, V.; ŠVARCOVÁ, I.; BUDIŠ, P.; LOEBL, Z.; PROCHÁZKOVÁ, B. *eGovernment bezpečně*. 1. vydání. Praha: Grada Publishing, a. s., 2008. 160 s. ISBN 978-80-247-2462-1.

[3] Smejkal, V. a kol. Právo informačních a telekomunikačních systémů. 1. vyd. Praha: C.H. Beck, 2001. 542 s. ISBN 80-7179-552-6.

Internetové zdroje:

[4] *Business.center.cz* [online]. 2010 [cit. 2009-11-23]. Dostupný z WWW: <http://business.center.cz/>.

[5] *BusinessInfo.cz* [online]. 2002 [cit. 2010-01-03]. Dostupný z WWW: <http://www.businessinfo.cz/cz/>.

[6] *Česká daňová správa* [online]. 2010 [cit. 2010-03-10]. Dostupný z WWW: <http://cds.mfcr.cz/cps/rde/xchg/cds/xsl/index.html?year=>.

[7] *Česká správa sociálního zabezpečení* [online]. 2010 [cit. 2010-04-13]. Dostupný z WWW: <http://www.cssz.cz/cz/novinky/>.

[8] *Daňový portál* [online]. 2010 [cit. 2010-04-10]. Dostupný z WWW: <http://adisepo.mfcr.cz/adistc/adis/idpr_pub/dpr/uvod.faces>.

[9] *EDI Zone* [online]. 2008 [cit. 2010-04-15]. Dostupný z WWW: <http://www.edizone.cz/>.

[10] *eIdentity, a. s.* [online]. 2010 [cit. 2009-12-20]. Dostupný z WWW: <https://www.eidentity.cz/Home.html>.

[11] *Ministerstvo vnitra České republiky* [online]. 2010 [cit. 2010-02-16]. Dostupný z WWW: <http://www.mvcr.cz/ministerstvo-vnitra-ceske-republiky.aspx>.

[12] *Podnikatel.cz* [online]. 2008 [cit. 2010-04-13]. Dostupný z WWW: <http://www.podnikatel.cz/clanky/elektronicka-fakturace-ma-zelenou/>.

[13] *Portál veřejné správy České republiky* [online]. 2010 [cit. 2010-02-16]. Dostupný z WWW: <http://portal.gov.cz/wps/portal/_s.155/710/place>.

[14] *PostSignum VCA* [online]. 2010 [cit. 2009-12-20]. Dostupný z WWW: <http://vca.postsignum.cz/>.

[15] *První certifikační autorita, a. s.* [online]. 2010 [cit. 2010-12-20]. Dostupný z WWW: <http://www.ica.cz/>.

[16] ROGALEWICZ, Jiří. Důvěryhodné uložení elektronických dokumentů. *Obec a finance, příloha Veřejná správa online* [online]. 2008, č. 5 [cit. 2010-04-13]. Dostupný z WWW: <http://vsol.obce.cz/clanek.asp?id=2008504>.

[17] *Úřední věstník* [online]. 2008 [cit. 2010-04-28]. Dostupný z WWW: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1999L0093:20081211:CS:PDF>.

Seznam zkratek

a. s. – akciová společnost

č. – číslo

ČR – Česká republika

DIČ – daňové identifikační číslo

DIS – daňová informační schránka

DPH – daň z přidané hodnoty

EDI - Electronic Data Interchange (elektronická výměna dat)

EPO – elektronické podání

EU – Evropská unie

FŘ – finanční ředitelství

FÚ – finanční úřad

I.CA – První certifikační autorita

IČ – identifikační číslo

MF – ministerstvo financí

PIN – personal identification number (osobní identifikační číslo)

Sb. – sbírky

s. p. – státní podnik

UN/EDIFACT - United National/Electronic Data Interchange for Administration Commers and Transport (pravidla OSN pro elektronickou výměnu dat ve správě, obchodě a dopravě)

USB – universal serial bus (univerzální sériová sběrnice)

VIES – VAT Information Exchange System (elektronický systém pro výměnu informací v oblasti DPH)

Prohlášení o využití výsledků bakalářské práce

Prohlašuji, že

- jsem byla seznámena s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě bakalářskou práci užít (§ 35 odst.3);
- souhlasím s tím, že jeden výtisk bakalářské práce bude uložen v Ústřední knihovně VŠB-TUO k prezenčnímu nahlédnutí a jeden výtisk bude uložen u vedoucího bakalářské) práce. Souhlasím s tím, že bibliografické údaje o bakalářské práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, bakalářskou práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne …….

……

jméno a příjmení studenta

Adresa trvalého pobytu studenta:
Poříčí 238, Solnice 517 01